# DATA BREACH POLICY

**Adopted Date:** 17 June 2026

**Policy Number:** GRC 108

**Policy Type:** Statutory

**Responsible Officer:** Chief Executive Officer

**Department:** Executive Office

| Version | Decision Number or CEO Approval | Decision Date | History |
|---|---|---|---|
| 1. | Adopted GRC 108 – OM-065/26 | 17 June 2026 | Review June 2029 |
| 2. | | | |

## Purpose

Goondiwindi Regional Council (Council) is committed to protecting personal information and responding appropriately to data breaches.

This policy establishes Council's framework for:

- Managing actual and suspected data breaches
- Complying with the Mandatory Notification of Data Breach (MNDB) scheme under the *Information Privacy Act 2009 (Qld)*
- Minimising harm to individuals and Council

## Scope

This policy applies to all personal information handled by Council, regardless of format, including:

- Information collected and stored in physical or digital formats
- Information accessed, processed or shared by contractors or service providers on behalf of Council
- All Council staff, councillors, contractors, consultants and volunteers
- Actual data breaches and suspected eligible data breaches

## Definitions

**Data Breach**: Unauthorised access to, or unauthorised disclosure of information or the loss of information in circumstances where unauthorised access to, or unauthorised disclosure of, the information is likely to occur in accordance with schedule 5 of the IP Act.

**Eligible Data Breach**: An eligible data breach will have occurred under section 47 of the IP Act where:

- there has been unauthorised access to, or unauthorised disclosure of personal information held by an agency, **and**
  the access or disclosure is likely to result in serious harm to any of the individuals to whom the information relates; **or**
- there has been loss of personal information held by an agency that is likely to result in unauthorised access to, or unauthorised disclosure of the personal information, **and**
  the loss is likely to result in serious harm to any of the individuals to whom the information relates

**Information Commissioner**: The Queensland Information Commissioner

**IP Act**: The *Information Privacy Act 2009 (Qld)*

**Serious Harm**: To an individual in relation to the unauthorised access or unauthorised disclosure of the individual's personal information, includes, for example:

- serious physical, psychological, emotional or financial harm to the individual because of the access or disclosure, or
- serious harm to the individual's reputation because of the access or disclosure

**Personal Information**: Information or an opinion about an identified individual or an individual who is reasonably identifiable from the information or opinion:

- whether the information or opinion is true or not, and
- whether the information or opinion is recorded in material form or not

**Policy Statement**

Council is committed to safeguarding personal information and will act promptly and transparently in the event of a data breach.

Council will:

- identify and respond to data breaches in a timely manner
- assess suspected eligible data breaches within required legislative timeframes
- notify the Information Commissioner and affected individuals where required
- take reasonable steps to contain and mitigate harm
- maintain appropriate records of all data breaches
- continuously improve its data breach management practices

Council will implement reasonable administrative, technical and physical safeguards to protect personal information from misuse, loss, unauthorised access, modification or disclosure.

**Responsibilities**

| Role | Responsibility |
|---|---|
| **Employee** | • Protect personal information in accordance with the IP Act<br>• Immediately report any suspected or actual data breach<br>• Cooperate with breach response activities |
| **Contractors & Service Providers** | • Immediately notify Council of any actual or suspected data breach involving Council information |
| **Manager** | • Ensure staff are aware of reporting obligations<br>• Escalate suspected data breaches appropriately |
| **Legal Officer** | • Coordinate the management of data breaches<br>• Assess suspected eligible data breaches<br>• Determine notification requirements<br>• Notify the Information Commissioner and affected individuals (as required)<br>• Maintain the Register of Eligible Data Breaches |
| **Directors** | • Provide oversight of significant data breaches<br>• Support resourcing and decision-making<br>• Convene a Data Breach Response Team where required |

| | |
|---|---|
| **Data Breach Response Team (DBRT)** | • Manage significant or high-risk data breaches<br>• Provide specialist advice and support response actions<br>• Team consists of (but not limited to):<br>  o Executive Team<br>  o Legal Officer<br>  o ITC Manager<br>  o Manager Cultural & Customer Service<br>  o Manager Community & Economic Development<br>  o Depending on the nature of the breach, the DBRT may need to include additional staff or external experts |

**Data Breach Management Framework**

Council manages data breaches in accordance with the following stages:

**Stage 1: Preparation**

Council will maintain appropriate policies, procedures and systems to support effective data breach management.

**Stage 2: Identification**

All suspected or actual data breaches must be reported to Legal Officer and assessed to determine appropriate escalation. Where the Legal Officer is unavailable or involved in the suspected breach, notifications must be made to the Chief Executive Officer or their delegate.

**Stage 3: Containment and Mitigation**

Council will take all reasonable steps to contain the breach and minimise potential harm. Immediate steps will be taken, where practicable, to contain the breach before full assessment is completed.

**Stage 4: Assessment**

A suspected eligible data breach arises where Council has reasonable grounds to suspect that an eligible data breach may have occurred. From this point, Council will take all reasonable steps to complete the assessment within required legislative timeframes.

**Stage 5: Notification**

Where an eligible data breach is identified, Council will notify the Information Commissioner and affected individuals as required under the IP Act. Notifications will include the information required under the Information Privacy Act, including details of the breach, the kinds of information involved and recommended steps individuals should take.

**Stage 6: Post data breach review and remediation**

Council will review all data breaches and implement improvements to prevent recurrence.

**Register of Eligible Data Breaches**

In accordance with section 72 of the IP Act, Council will maintain:

- a Register of Eligible Data Breaches and
- an internal Data Breach Register capturing all actual and suspected breaches

**Record Keeping**

Council will maintain records of all data breaches, in Council's Internal Data Breach Register including:

- Details of the incident
- Actions taken
- Assessment outcomes
- Notification decisions

All complaints relating to possible breaches of privacy will be managed through formal procedures, as detailed in the Complaints Process Policy.

**Related Legislation and Policies**

- *Information Privacy Act 2009 (Qld)*
- *Information Privacy and Other Legislation Amendment Act 2023* (IPOLA)
- *Right to Information Act 2009 (Qld)*
- Queensland Privacy Principles (QPPs)
- GRC 045 Information Privacy Policy
- GRC 017 Complaints Management Policy
- GRC Data Breach Response Plan

**Review**

June 2029